Road map for Enterprise Risk Management
Enterprise Risk Management (ERM) Roadmap

ERM has come full circle in some ways. When ERM began to take shape in the 1990's, the focus was on improving financial performance. The consulting community that grew up around ERM struggled to get traction with it until some high-level business failures (Enron, Anderson Consulting etc.) brought on regulatory changes such as Sarbanes Oxley and others that provided a high level of motivation for publicly traded companies to adopt ERM. The consulting community took full advantage of this new regulatory environment and ERM took on a very compliance oriented approach. However, in time many of the ERM practices started in this compliance environment became stale, checklist type functions and lost momentum. The value didn’t seem evident. During the last few years there has been a movement back toward “Strategic Risk Management” which is focused more on strategy and improving financial performance. COSO has recently done a major revision of its’ ERM Framework recognizing this trend. Our approach to the ERM roadmap is completely consistent with this trend and we believe our process is more effective given our “lean” approach and focus on risk bearing capacity and decision making.

We built the USI ERM roadmap from ground-up and adjust it to the clients’ culture based upon their input, rather than using an off-the-shelf template. We begin with a few premises:

1) Risk and opportunity are value judgments applied to uncertainty and such value judgments can only be made in the context of goals or objectives – i.e. a desired outcome that is uncertain.
2) Therefore, risk and opportunity are always linked around specific objectives.
3) Without risk, there is no opportunity (risk is good!).
4) So, taking risk is an essential need of every organization seeking to profit or achieve some objective of value.
5) This places a high value on an organization’s financial capacity to take risk, which is limited by the organizations financial size and condition. Therefore, utilization of risk bearing capacity must be weighed against opportunities that have the highest potential importance or value to the organization.
6) The impact of risk on any organization is the collective impact of all risks acting together in each fiscal period.

ERM is the process of improving risk-related decision-making to support achievement of organizational objectives by addressing the full spectrum of risks and managing them as an interrelated portfolio. It’s a process for identifying risks and opportunities across the enterprise, making well thought-out risk/reward decisions, taking actions to mitigate necessary risks and communicating what we learn across the organization.

It is important to keep the focus on the true goal of ERM, which is to improve risk related decision making in a consistent way across the organization. Risk identification, assessment, quantification and mitigation, while important, are all subordinate functions. ERM should enable individuals to make better decisions, weighing risk and reward before actions are taken and resources are allocated such that they increase their success in achieving objectives for which they are accountable and which bring value to the business. Having helped many different types of organizations implement ERM, we have learned that ERM must be individually rewarding to such decision makers for them to become engaged. Once people are engaged, ERM becomes self-sustaining.

To improve risk related decision making, there must be an understanding of the organization’s financial capacity to take risk and management’s willingness to use that capacity to achieve some goal. ERM must enable a decision-maker to differentiate between a good risk/reward trade-off and a bad one from the perspective of senior leadership. But ERM can’t become the “nay-sayer” in the process if it is going to succeed. ERM must always help the decision-maker “get to yes” by helping to manage or mitigate the risk whenever possible such that the decision to proceed becomes a good risk/reward trade-off rather than a bad one.
## ERM Roadmap Overview

Our ERM roadmap uses a 7-step approach:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Kick-off meeting</td>
<td>Define goals and objectives, Define roles, Define Risk Bearing Capacity, tolerance and appetite</td>
</tr>
<tr>
<td>Step 2</td>
<td>Risk Bearing Capacity Analysis</td>
<td>Review a series of hypothetical amounts of loss, each with well-defined business consequences, to identify client’s threshold of risk tolerance</td>
</tr>
<tr>
<td>Step 3</td>
<td>Risk assessment</td>
<td>Establish standard scales for rating frequency, severity and vulnerability, Work with key stakeholders to identify and assess risks throughout the client organization</td>
</tr>
<tr>
<td>Step 4</td>
<td>Validation and prioritization of findings</td>
<td>Assemble findings in a corporate risk register, Conduct a workshop to validate interview findings, Prioritize the top 10 ~25 risks and map them by frequency and severity</td>
</tr>
<tr>
<td>Step 5</td>
<td>Deeper analysis and scenario planning</td>
<td>Work with business units on deeper analysis of top risks, Assess and develop mitigation tools</td>
</tr>
<tr>
<td>Step 6</td>
<td>Forecast potential aggregate impact of risk against risk tolerance</td>
<td>Create a reasonable estimate of the likelihood and potential impact of identified risks in the aggregate to the client’s business, Compare exposure to limit of risk tolerance identified in step 2</td>
</tr>
<tr>
<td>Step 7</td>
<td>Develop a simple ERM governance structure</td>
<td>Establish ERM steering committee and operating protocols, Embed ERM into existing business decision making processes, Incentivize decision maker engagement</td>
</tr>
</tbody>
</table>
ERM Roadmap

Step 1

We will prepare a kick-off meeting with senior leaders who will be involved in the project to ensure we have their agreement with our overall approach, understand their roles and the results we are seeking as the roadmap is deployed. To ensure consistency in the way decisions are made across the organization it is also important to agree on a formal definition of the terms risk bearing capacity, risk tolerance and risk appetite. We define these terms as follows:

- Risk bearing capacity (RBC): An organization’s overall financial capacity to take risk
- Risk tolerance: The limit of risk bearing capacity within which management wishes to operate the business
- Risk appetite: Management’s willingness to use that financial capacity to achieve an objective

USI’s systematic approach builds on business strategy, demand for capital, capital structure, and Risk Bearing Capacity to create an analytical framework that drives the design of risk solutions and supports decision making.
Step 2

To help further define RBC and Risk Tolerance, we look at a series of benchmarks (hypothetical amounts of loss) that, if experienced in a given timeframe, would result in well-defined business consequences. It is helpful to begin with the amount of financial loss that would put the organization on the brink of insolvency as it reinforces the idea that RBC is finite. Then, other benchmarks such as violating loan covenants, a downgrade in credit rating or inability to fund strategy as planned can be examined. Given this continuum of benchmarks with clearly defined business consequences, a company’s senior executives are better able to agree on a level of risk tolerance within which they would manage the business.

Step 3

Risk assessment. Through a series of meetings, the team will work with key stakeholders to holistically assess risks throughout the organization. Standard scales for rating frequency, severity and vulnerability will be established with senior leaders based on step 2 so they can be applied consistently across the organization. The team will interview senior leaders, key staff functions (Finance, HR, IT, Risk Management, Legal etc.) and key business-unit leaders about risks that might prevent them from achieving their objectives.

- What are those risks?
- If they materialized, how would they impact both the individual business units and the rest of the company? What impact would they have on people, revenue, net income, cash flow, brand/reputation or customers?
- What is the estimated likelihood and potential impact of each risk?
- How well are business units currently managing the risks? How vulnerable is the business given current controls? Are there opportunities to improve?
- How rapidly will the impact of the risk be realized by the business?
- Are these risks correlated with other risks? In what way?

The inverted risk assessment pyramid illustrates the dimensions in which risks should be evaluated:

- Impact is potential severity
- Velocity is the speed with which the risk materializes
- Likelihood is frequency
- Vulnerability includes aspects of operations or the environment that make the risk more or less likely or severe
- Correlation is the relationship between this risk and other risks
- Complexity increases the capability of a system but may reduce its predictability
Step 4

After the interviews, the team will record the findings from each business unit and assemble the findings in a corporate risk register that captures the risks, impacts, likelihoods, and vulnerability. From this register, the team will conduct a validation workshop with a smaller, diverse, cross functional team to validate the interview findings and prioritize the top 10 - 25 risks that have the greatest potential to impact the organization to be the focus of mitigation planning. We will also look at potential correlations between risks in this phase. The team can further assist with preparation of a report for board reporting purposes.

Step 5

Once the assessment is complete, the team will work with the business units on a deeper analysis of the top risks. This phase involves scenario-planning for each critical risk, including assessment of mitigation tools and possible development of new ones. The team can assist in modeling to show how events correlate across different risk scenarios and help business leaders make better risk-adjusted decisions.
Step 6

It is also important for management to have a reasonable estimate of the likelihood and potential impact of existing strategic and other uninsurable risks, as these risks must be supported by the organization’s balance sheet and consume some portion of the company’s agreed upon risk tolerance. Understanding how much of that capacity is consumed by such risks and how much is left within the established risk tolerance establishes whether the company has “surplus” capacity to take other risks and enables management to make better judgments about how to value risk-reward tradeoffs going forward.

The chart below shows a confidence interval analysis of the risks identified in the ERM process (ERM Risks) compared to the historical volatility of the client’s EBITDA and the EBITDA volatility experienced by their peer group. We often find correlations between these different sets of data, giving us greater confidence that our estimates of the likelihood and severity of ERM risks in the aggregate are in line with the historical experience of both the client and peers. The RBC line indicates the client’s chosen risk tolerance. In this example, the client has “surplus risk bearing capacity” available to take other risks deemed beneficial to the organization. Please see our first case study below to learn more about this analysis.
Step 7

Finally, the team will work with the internal ERM leaders and other top stakeholders to develop a simple ERM governance structure to oversee the ERM process and embed it into decision making within existing business processes. The most impactful decisions are made in relation to functions like strategic planning, budget and capital expenditure approvals where an action is being chosen and resources are being allocated to it. Asking if we have identified, assessed and quantified risk in deciding on the action and determining what resources are required is a very natural part of that process and ERM enables this to be done in a more systematic, consistent and effective way. Further, by embedding ERM in these existing functions, we avoid creating new bureaucracy which can be a serious ERM killer. The role of the ERM leader and steering committee is to make sure these functions have the tools and resources they need to incorporate the ERM process into their broader function, collect the risk information derived from the process, share best practices and report progress to all stakeholders. We can help establish reporting protocols so knowledge is shared widely throughout the organization. This process helps create visibility of risks and mitigation strategies throughout the enterprise and at the board level.

It is our intent at each step of the process to help the client internalize this process so it can be sustained without outside assistance when you are ready to take it over.

Our approach is very straight forward and seeks to embed ERM into other existing business practices in the least intrusive way possible while still meeting the goal of improving risk related decision making. As such, it can be seen as a “lean” form of ERM.

Our case studies outline some key successes of our ERM roadmap:

The first case study demonstrates our analytical capabilities:

- We met with ABC to review the internal work ABC had done identifying and assessing enterprise risks. We identified a set of 37 risks for which estimates of frequency and severity were established and performed a Monte-Carlo simulation analysis on these risks to provide an estimate of their potential impact to ABC at various confidence intervals.
- In addition, we performed a peer analysis using ten years of data on EBITDA for ABC and each of ten peer companies. Our objective was to measure the volatility of EBITDA over the ten-year period for both ABC by itself and the peer group as a whole to estimate the potential impact of strategic and other uninsured risk to ABC’s EBITDA if they experienced the same volatility as the peer group.
- We found a high degree of correlation between the results of the Monte-Carlo analysis and the peer EBITDA over 10 years at a 95% confidence interval, giving us reasonable confidence in an estimate of $300 million for strategic and other uninsured risks.
- We then helped ABC estimate their financial capacity to take risk, or Risk Bearing Capacity (RBC). The client decided that a violation of their lending covenants could have a significant adverse impact on their ability to execute their business strategy going forward and chose this business consequence as their maximum threshold of risk tolerance or RBC. We calculated that a loss of $450 million could be sustained before the covenants were breached.
- With an estimate of $300 million representing the potential impact of strategic and other uninsured risks to their business at a 95% confidence interval and their ability to withstand a $450 million loss before breaching their loan covenants, it was reasonable to estimate that they had “surplus” or additional capacity to sustain a loss up to $150 million.
- Two years later, ABC internally reviewed and revised their key risk register. In addition, ABC refinanced and modified their debt structure. We were asked to repeat our analysis based on ABC’s revised key risk register, to establish an estimate of the potential impact to ABC of strategic and other uninsurable risks for the purpose of providing additional insight into ABC’s liquidity needs in the context of their new capital structure. While risks had increased in potential impact, we found high correlation once again between the peer analysis and the Monte Carlo analysis of their risk register. Risk Bearing Capacity had also increased in the context of their new capital structure giving them higher overall surplus capacity for risk.
Case study 2 demonstrates our risk identification practices:

- The ERM assessment process involved interviews with 15 senior managers representing all major corporate departments and resulted in identification and preliminary quantification of 40 risks. These 40 risks were further re-evaluated in a validation workshop conducted with a cross section of 6 senior managers in which estimates of likelihood and potential impact from the original interviews were discussed and voted on by the validation team for purposes of prioritization. Ten risks were found to have the highest combination of likelihood and potential impact.

- The quantification of these risks is preliminary as they were based on the perceptions of the interviewees and validation team without in-depth effort to quantify impact and probability in detail. If management agrees with the top 10 issues, then further efforts will be made to refine these estimates and establish metrics to measure the effectiveness of the mitigation strategies developed in response to these risks, which is the next step in the ERM process.

The scales used for preliminary quantification are as follows:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Likelihood</th>
<th>Impact - $</th>
<th>Impact - qualitative</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Once in 20 years or more (5%)</td>
<td>Material = $</td>
<td>Requires unexpected interruption/intervention of senior executives</td>
<td>Highly effective controls in place</td>
</tr>
<tr>
<td>2</td>
<td>Once in 15 years (25%)</td>
<td>Moderate = $</td>
<td>Potential for adverse publicity/minor injury</td>
<td>Good controls in place, some improvement possible</td>
</tr>
<tr>
<td>3</td>
<td>Once in 10 years (50%)</td>
<td>Significant = $</td>
<td>Potential legal or regulatory issues</td>
<td>Moderate level of control, good opportunity for improvement</td>
</tr>
<tr>
<td>4</td>
<td>Once in 5 years (75%)</td>
<td>Serious = $</td>
<td>Potential adverse impact to brand or reputation</td>
<td>Controls are limited, excellent opportunity to improve</td>
</tr>
<tr>
<td>5</td>
<td>Every year or more (95%+)</td>
<td>Catastrophic = $</td>
<td>Potential serious injuries to the public and/or employees</td>
<td>Few or no controls in place</td>
</tr>
</tbody>
</table>

- The risk register and map graphically display the top risks using all three criteria. Vulnerability is represented by the size of the bubble with impact on the vertical axis and likelihood on the horizontal. (See the sample chart in step 4 as an example).

- We further identified common threads between key risks that suggest possible correlations and provided insight into potential methods of mitigation.

The ERM roadmap is a way of learning how you can better differentiate your company from your competitors by doing a continuously improving job of managing risk. Studies have shown that companies that rank in the top 20% on ERM maturity outperform others significantly in the growth of revenue, cash flow and enterprise value. This finding, in our opinion, isn’t simply because they do ERM well. It is because by doing ERM well they also learn to do a lot of other things better that together improve the performance of the business.

ERM programs often get stuck because they focus on risk identification, assessment and mitigation as the goal. Quantification is difficult for many risks and people become disillusioned when they can’t measure something. The process becomes a “check the box” list of things they must manage better, but they can’t really measure what they are doing in terms of positive or negative impact to the business and the process stalls out. We focus on helping people with quantification to overcome this hurdle.
Some of the other things that cause ERM to fail include:

- Failure to get executive sponsorship. Embracing enterprise risk management must start at the top and end as a valued part of ordinary business management.
- Holding on to silos. Risk management should be integrated across all departments.
- Lack of awareness. Leaders should understand how their business-unit risks can impact the entire enterprise.
- Lack of incentives. ERM cannot work if employees get penalized for making good risk-based decisions.
- Outdated assumptions. ERM is a tool for making decisions based on real-time business facts and emerging information.
- Lack of ownership. For ERM to work, business units must own the identified risks and mitigation efforts that roll up to board-level reporting.
- Forgetting to monitor. ERM requires ongoing governance and measurement of risk-mitigation tools and strategies.
- Adding layers of new bureaucracy to support ERM tends to bog things down, slows decision making and reduces overall enthusiasm for ERM.

The key ideas that differentiate the USI ERM roadmap include:

- Risk and opportunity are value judgments applied to uncertainty and such value judgments can only be made in the context of goals or objectives – i.e. a desired outcome that is uncertain. Risk and opportunity are always linked. Risk is good.
- We believe that a company’s financial capacity to take risk and the ability to make thoughtful risk related decisions are critical components of its ability to create value for shareholders.
- Defining and communicating a clear understanding of the firm’s risk bearing capacity, tolerance and appetite to all decision makers across the business together with the habit of assessing the risks associated with their decisions will improve performance.
- Companies that practice ERM successfully learn to take risks intelligently, with eyes wide open. ERM is a continuous learning process that adds value to the business.
- ERM must be individually rewarding to decision makers for them to become engaged.

The key to sustained success is getting decision makers engaged. If they see ERM as helping them “get to yes”, i.e. finding ways to take risks that enable them to achieve their objectives within the risk tolerance and appetite established by senior management, then they will engage and keep the ERM practice vital, alive and self-sustaining.